Compliance Guidelines for FISMA and FIPS

Audience:
CIO, COO, IT, security, risks managers in government organizations
Business problem:
How can government agencies meet full compliance with the Federal Information Security Management Act (FISMA) and Federal Information Processing Standards (FIPS)?
Technology focus:
Intrusion detection and vulnerability assessment
Point of view:
An explanation of how government agencies can pass FISMA audits to determine that protections of information assets meet Federal Information Processing Standards

Abstract:
With the passage of the Federal Information Security Management Act (FISMA) in 2002, government agencies are no longer allowed to waive mandatory Federal Information Processing Standards (FIPS). These agencies must now report their level of compliance and be prepared for audits by the internal Inspector General's office or by external auditors. In this presentation, the speaker will describe intrusion prevention and vulnerability management techniques that can help government agencies comply with FIPS, as mandated by FISMA. He/she will outline a layered approach to infrastructure security that provides comprehensive protections, as recommended by the National Institute of Standards and Technology (NIST). The session shows how government agencies can shield sensitive data; track the blocking of hacker attacks, and implement network vulnerability management with automated repair workflow reporting.

Attendees will learn:
- Minimum information security requirements as mandated by FIPS and FISMA
- How government agencies can address constant hacker threats while keeping networks connected to the Internet fully operational
- Best practices for layered defense at the perimeter, network, workstation, application and data levels
- How to continually monitor the infrastructure for any vulnerability risk with automated reporting on system repairs
- How automated intrusion prevention and vulnerability management can streamline IT administration, resulting in lower costs and higher effectiveness

Speaker Biography:
Mitchell Ashley
Vice-President Engineering and CIO
StillSecure
361 Centennial Parkway, Suite 250
Louisville, CO 80027
PH: 303-381-3848

As Vice President and CIO of StillSecure, Mitchell Ashley is responsible for the product strategy and development of a suite of network security software.... Has more than 20 years' experience in data networking, network security and software development.... Prior to joining StillSecure, Mitchell was Vice President of Engineering and CIO at Jato Communications, where he directed the design and build-out of secure access data networks, information systems, and managed customer service operations... Mr. Ashley has also held leading positions in the industry as a co-founder of BoldTech Systems, a Denver-based distributed applications consulting firm.... With US West Advanced Technologies, he led the creation of interactive video, entertainment and data network applications... Worked with Electronic Data Systems where he designed and built scalable, integrated systems in the banking and telecommunications industries... Holds a Bachelor of Science degree in computer science and business administration from University of

Nebraska at Kearney... Member of Association for Computing Machinery (ACM), Information Systems Security Association (ISSA), and American Bar Association (ABA).... Frequent speaker at industry events, including ISACA conferences; DSL ComForum and DSL World; and Macworld; and was a seminar instructor and a member of technical journal editorial board at Electronic Data Systems.

About StillSecure (www.stillsecure.com)
StillSecure provides affordable, easy-to-use network security software products for IT and security professionals at security-conscious enterprises. The StillSecure suite reduces the risk and liability of damages from network attacks and tangibly increases the productivity and effectiveness of your resources. StillSecure is available through Latis Networks' direct sales force and channel partners. Latis Networks is financed by Mobius Venture Capital, 3i, and Feld Group Ventures.